REMARKS/ARGUMENTS

Claims 1-21 are now in the application. Claims 1-17 have been amended, and claims 18-22 have been added. Applicants respectfully request reconsideration of the application, as amended, in view of the following remarks.

Applicants wish to thank Examiner Kiss, Examiner Ingberg, and the Patent Office for the personal interview on January 19, 2006.

Applicants have amended the drawings and the specification to address the Examiner's objections and rejection. Applicants have amended paragraph [0112] to include the following new reference numbers for Figure 12: reference numbers 150, 152, and 154 refer to the rectangles; reference numbers 156, 158, 160, and 162 refer to the ovals; and reference numbers 164, 166, 168, 170, 172, 174, 176 and 176 refer to the arrows. The Replacement Sheet for Figure 12 showing those reference signs is attached hereto. The Replacement Sheet for Figure 1 shows reference signs 10, 12, 14, 16, 18, and 20, and the Replacement Sheet for Figure 13 shows the reference signs 134, 136, 138, 140, 142 and 144.

Applicants have amended the specification to incorporate by reference the contents of provisional patent application Serial No. 60/464,019, to which the present application claims priority under 35 U.S.C. §119(e).

Claims 1-17 have been rejected under 35 U.S.C. §101. As further discussed below in relation to the Wagner et al reference, Applicants have amended the claims to clarify that (a) their invention is directed to a *computer implemented* method and utility for detecting

vulnerabilities, and (b) their method and utility includes *the generation of a report which ranks the vulnerabilities as a function of the analysis.* Consequently, Applicants believe the claims are directed to proper subject matter under 35 U.S.C. §101.

Claims 1-17 have been rejected under 35 U.S.C. §102(b) as being anticipated by David Wagner, et al., " A First Step Toward Automated Detection of Buffer Overrun Vulnerabilities," Proceedings of the Network and Distributed System Security Symposium, Feb. 2000 (hereinafter, Wagner et al.)

Wagner et al uses constraint language and formal methods to detect the existence of buffer overflow vulnerabilities in C source code. Wagner et al converts C source code into a constraint language, and analyzes the constraint language to determine the existence of buffer overflow vulnerabilities.

In contrast to Wagner et al, the claimed invention uses compiler techniques, as opposed to constraint language and formal methods, to detect vulnerabilities. The claimed are directed to a computer implemented method and utility for analyzing computer-executable source code in the context of the source code's inherent control flow and data flow. All of these features are found in independent claims 1, 15 and 16. Therefore, these claims and all their dependent claims should be found allowable.

In addition, the claimed method and utility is not part of the compiler for the program that is being analyzed, but rather is a separate method and utility which is used to identify the vulnerabilities in a pre-existing computer program. Furthermore, the analysis is conducted in the computer-executable source code, and not in annotations to the source code. The method and utility generates a report to identify the vulnerabilities.

The claimed invention offers many advantages, including the potential to identify the locations in the source code that cause the vulnerabilities, and the ability to identify all types of vulnerabilities in all types of programming languages. Wagner admits to shortcoming in these areas: it cannot identify the place in the code where the vulnerability arose (page 11, col. 1, lines 26-27); it is limited to detecting only buffer overflow vulnerabilities (page 2, col. 2, lines 10-11); it works only with C code (page 2, col. 2, lines 10-11); and it identifies many false positives (page 2, col. 2, lines 21-24). Thus, Wagner et al not only fails to anticipate the invention, but teaches away from it.

In addition, the dependent claims present a number of novel features as well. For example, dependent claims 18 and 19 are directed to the use of a data base having information about routine calls, including information about one or more specified conditions that can present a vulnerability. The method and utility uses the data base to retrieve information for a routine call to check for a specified condition to see whether the routine call will present a vulnerability. In addition, the claimed invention generates a report which identifies the place in the code where the vulnerability occurred. This feature is found is in dependent claims 20, 21 and 22.

Applicants attempted to capture the features described above in the original claims, but it seems that those claims may have received an unintended interpretation. Applicants believe that the present amendments will avoid the unintended interpretations and should make these distinctive aspects more apparent.

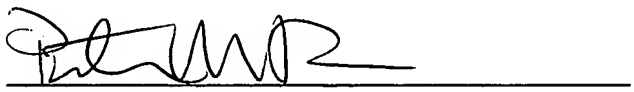
For the reasons stated above, we believe that the claims are allowable.

Applicants are in the process of gathering reference citations in order to finalize an Information Disclosure Statement. Applicants will submit that Information Disclosure Statement to the Patent Office promptly.

The Commissioner is hereby authorized to charge the required fee of $225.00 for filing the request for extension of time to our Deposit Account No. 08-0219. Please apply any charges not covered, or any credits, to Deposit Account No. 08-0219.

Respectfully submitted,

Date: 2/7/06



Peter M. Dichiara
Reg. No. 38,005

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, MA 02109
Telephone: (617) 526-6466
Facsimile: (617) 526-5000